



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,776	11/15/2001	Esa Turtiainen	032986-019	4500
27045	7590	02/22/2006	EXAMINER	
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR C11 PLANO, TX 75024			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/003,776

Applicant(s)

TURTIAINEN ET AL.

Examiner

Shewaye Gelagay

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 19 January 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 19, 2006 has been entered.
2. Claims 1-7 are pending.

### ***Response to Arguments***

Applicant's arguments regarding Mamros or Patel do not teach "modifying the second security association by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first node and second nodes" with regard to claims 1 and 5 have been considered but are moot in view of the 35 U.S.C. 112 rejections given below. Applicant's argument regarding claims 2 and 7 Mamros or Patel do not teach "streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload headers (ESP)" is persuasive but is moot in view of the new ground(s) of rejection.

### ***Specification***

3. The disclosure is objected to because of the following informalities: The disclosure has Figure 6 on page 7 second paragraph, however, the drawing has only Figures 1-5. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1 and 5 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 1 and 5 recite "modifying the second security association (SA2) by using selected components of the second protocol". The Applicant teaches entering IKE phase 2 and negotiating a pair of IPSec SAs data relevant to encryption, including a pair of encryption keys and using IKE phase 2 each time a new connection is required. The Examiner would like to point out that nowhere does the Applicant teach "modifying the second security association (SA2) by using selected components of the second protocol" in the application as filed.

6. Claims 2-4 and 6-7 depend from respective claims 1 and 5, hence inherit the deficiencies of claims 1 and 5, respectively.

Art Unit: 2137

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 2-4 and 6-7 depend from respective claims 1 and 5, hence inherit the deficiencies of claims 1 and 5, respectively.

9. Claims 1 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1 and 5 recite "using the first protocol to establish a first security association (SA1) over a second protocol between the first and second nodes". The limitation is ambiguous. It has been already disclosed in the previous limitation that a first protocol is used to establish SA1. It is unclear how a second protocol is used in establishing SA1. Applicant has not explained how the same SA1 is established by using the first protocol over a second protocol. It is unclear whether the first protocol or the second protocol is used in establishing SA1.

Appropriate correction is required.

10. Claims 2-4 and 6-7 depend from respective claims 1 and 5, hence inherit the deficiencies of claims 1 and 5, respectively.

11. Claims 1 and 5 recite the limitation "the second security association (SA2) " in line 8. There is insufficient antecedent basis for this limitation in the claim.

### ***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2137

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269 in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel).

As per claims 1 and 5:

Mamros teach a method of sending streamed data over an IP network from a first node to a second node, the method comprising:

using a first protocol to establish a first security association (SA1) between the first and second nodes; (Col. 6, lines 9-13)

using a first protocol to establish a first security association (SA1) over a second protocol between the first nodes and second nodes; (Col. 6, lines 9-13)

modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first and second node; (Col. 6, lines 2-3; *for examining purposes modifying the second security association is interpreted as entering IKE phase 2 and negotiate a pair of IPSec SA data including a pair of encryption keys based on the description given in the specification, Page 6, paragraph 3*)

Art Unit: 2137

constructing datagrams containing segments of the encrypted streamed data in the datagram payload, the datagrams including a reduced overhead corresponding to the selected components; (Col. 5, lines 51-67 and Col. 6, lines 1-7) and

sending the datagrams from the first node to the second node. (Col. 2, lines 44-45; Col. 3, lines 15-30 and lines 45-47)

In addition, Mamros discloses sending encrypted streamed data. (Col. 1, lines 66-67 and Col. 2, line 1; Col. 6, line 2). Furthermore, Mamros disclose establishing secure and authenticated channel using ISAKMP/Oakley protocol. (Col. 6, lines 8-22)

Mamros does not explicitly disclose using first protocol to establish security association between the first node and second nodes and second protocol for providing encryption at the first node

Patel in analogous art, however, discloses using phase 1 negotiation (*is interpreted as the first protocol, the interpretation is given based on description given in the specification, page 6, paragraph 2*) to establish first security association (SA1) between the first node and second nodes (Page 1, paragraph 5; Page 2, paragraph 1) phase 2 negotiations (*is interpreted as the second protocol, the interpretation is given based on description given in the specification, page 6, paragraph 3*) for providing encryption at the first node. (Page 1, paragraph 5; page 2, paragraph 1)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros to include using phase 1 negotiation to establish security association between the first node and second nodes and phase 2 negotiations for providing encryption at the first node. This

Art Unit: 2137

modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Patel (Page 2, paragraph 2) in order to reduce a startup time for communication and improve the efficiency of the protocol.

As per claim 3:

Mamros and Patel teach all the subject matter as discussed above. In addition, Mamros further discloses a method wherein said first and second nodes are end points for the data. (Figure 1; Col. 3, lines 27-29)

As per claim 4:

Mamros and Patel teach all the subject matter as discussed above. In addition, Mamros further discloses a method wherein said first and second nodes tunnel data between respective end points. (Figure 2; Col. 3, lines 27-29)

As per claim 6:

Mamros and Patel teach all the subject matter as discussed above. In addition, Mamros further discloses an apparatus, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC). (Figure 2; Col. 3, line 15)

14. Claims 2 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269 in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel) further in view of Dutnall United States Letter Patent Number 6,584,098.



Art Unit: 2137

As per claim 2:

Mamros and Patel teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.

Dutnall in analogous art, however, discloses a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. (Col. 13, lines 22-28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros and Patel to include a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Dutnall (Col. 3, lines 51-52) in order to avoid excessive delay to a voice signal by reducing significant extra processing overhead.

As per claim 7:

Mamros and Patel teach all the subject matter as discussed above. In addition, Mamros further discloses an apparatus, the apparatus being a firewall or gateway

Art Unit: 2137

coupled to the first node which is the source of the streamed data. (Figure 2; Col. 3, line 23)

Both references do not explicitly disclose a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.

Dutnall in analogous art, however, discloses a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. (Col. 13, lines 22-28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros and Patel to include a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Duntall (Col. 3, lines 51-52) in order to avoid excessive delay to a voice signal by reducing significant extra processing overhead.

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay  
2/17/06



EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER